How Grades Were Assigned

Grades are primarily based on the percentage of mission-critical systems that Federal departments and agencies reported were Year 2000 compliant on August 13, 1999. Federal departments and agencies reporting 100 percent of their mission-critical systems Y2K compliant on August 13, 1999, earned a base grade of "A." Agencies with a base Y2K compliance rate of 99 percent earned a "B." Those with base compliance rates of 94 percent to 98 percent earned a "C," and 89 percent or lower earned an "D." Agency program completion dates influenced overall program grades.

The Y2K compliance rate is a significant factor in evaluating Y2K performance. But the subcommittee also considers other important factors, which raise or lower base grades. They are:

1. Contingency Plans – Agencies should have most of their basic contingency plans in place. Many have made the fundamental error of preparing contingency plans only for systems they know will be late. The subcommittee and the General Accounting Office expect agencies to prepare contingency plans that will allow them to continue their basic operations, assuming there will be system failures. These plans are called "business continuity and contingency plans." Draft plans were due to the President's Office of Management and Budget on June 15, 1999.

2. Telecommunications Systems – In-house private branch exchanges (PBXs), local area networks/wide area networks (LAN/WAN), and commercial switched networks are all vulnerable to Year 2000 problems. By now, all agencies should have completed a thorough inventory and assessment of all telecommunications systems. A high percentage of these systems should already be Y2K compliant, and a realistic plan should be in place for those that are not.

3. Embedded Systems – Microprocessor chips of various types are often built into, or embedded, in control devices. They might read magnetic strips in security badges or measure such basic things as how many gallons of water flow through a pipe per minute. Many embedded chips have no overt date dependency, but nonetheless use date-related calculations. Unfortunately, the only way to know whether an embedded chip is compliant is to test it. By now, agencies should have a complete inventory of all embedded chips, know whether most of them are compliant, and have a remediation plan in place for those that are not.

4. External Data Exchange – Most computers exchange data with other computer systems. External data that is not Y2K compliant can easily corrupt computer systems that are Y2K compliant. Agencies should have a complete inventory of their data exchanges, with emphasis on external exchanges. They should know which exchanges are compliant, and they should have a plan in place for those that are not.

5. Verification Efforts — Having a "second set of eyes" to independently assess the readiness of computer systems is a sound management practice. In their quarterly report to the Office of Management and Budget, agencies report independent verification activities to assure that systems are fixed and that information reported is accurate.

6. Percentage of Renovated Systems – The President established the date of March 31, 1999, for agencies to complete renovations of their mission-critical systems. If an agency failed to meet that milestone and its current percentage of renovated systems is low, it may be assumed that the agency could have difficulty completing all system-related work in the fall.

7. Strong Management Involvement – If senior executives within an agency or department demonstrate significant involvement in Year 2000 activities, that leadership role is considered a positive factor in the overall assessment.

8. Heavy Reliance on Replacing Systems – The Federal Government generally has a very poor track record of implementing new systems on time and within budget. As a result, the base grade was lowered if a department or agency reported replacing a high percentage of its mission-critical systems.

Of note, the accompanying spreadsheets provide data on the Federal Government's "high impact programs." These programs were deemed ready if agencies reported that operational tests among all business partners' systems were complete and if business continuity and contingency plans had been developed.